NPS-IS-14-001

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SUSTAINMENT AND NET-READY KEY PERFORMANCE PARAMETERS (KPP) IN AN ENTERPRISE INFORMATION SYSTEM (EIS) VALUE ASSURANCE FRAMEWORK (VAF)

by

C.R. Gunderson

April 2014

Approved for public released; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
23-04-2014	Technical	1 Oct 13 – 30 Sept 14

4. TITLE AND SUBTITLE
Sustainment and Net-ready Key Performance Parameters (KPP) in an Enterprise Information System (EIS) Value Assurance Framework (VAF)

5a. CONTRACT NUMBER
HHM402-13-1184

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR

Christopher R. Gunderson

5d. PROJECT NUMBER
RFGK4

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Christopher R. Gunderson
Dept of Information Science
Naval Postgraduate School
Monterey CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

NPS-IS-14-001

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
John Snevely
Office of the Undersecretary of Defense for Intelligence
1400 Defense Pentagon
Washington, DC 20301

10. SPONSOR/MONITOR'S ACRONYM(S)
OUSD(I)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Enterprise Information System (EIS) Value Assurance Framework (VAF) is an Information Technology (IT) governance model based on commercial best practice adapted to specific DoD and Intelligence Community (IC) acquisition policy requirements. VAF expands and abstracts traditional DoD "Availability" metrics such as "Operational Availability" A_o to develop objective time-based Key Performance Parameters (KPP) appropriate for software-intensive systems of systems. In particular VAF addresses both the DoD "Sustainment KPP" (S-KPP) and the "Net-Ready KPP" (NR-KPP). Hence, VAF provides an engineering assurance model for developing systems that deliver sustainable information superiority. In the VAF construct, the NR-KPP correlates measurable improvement in "Information Processing Efficiency" (IPE) to measurable improvement in traditional operational effect metrics such as Probability of Kill (Pk). In addition to that focus on operational efficiency, VAF recognizes that sustainment of modern IT systems requires process-level metrics that enforce speed-to-capability requirements. Hence VAF S-KPPs specify both threshold and objective speed-to-capability requirements commensurate with "Moore's Law." To achieve aggressive speed-to-capability, the VAF S-KPPs emphasize re-use of pre-certified COTS and GOTS components. The VAF addresses both of these types of KPPs through a recommended iterative process, consisting of 10 steps. Applying this process to a notional coalition counter-insurgency mission thread demonstrates its viability.

15. SUBJECT TERMS
Agile acquisition, network systems engineering, open system approach, OSA, service oriented architecture, net-ready key performance parameter, KPP, 6212, netcentric, network centric, information centric, enterprise information system

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			C.R. Gunderson
Unclassified	Unclassified	Unclassified	UU	39	**19b. TELEPHONE NUMBER** ***(include area code)*** 831 224 5182

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route
President

Douglas A. Hensler
Provost

The report entitled *"Sustainment and Net-ready Key Performance Parameters (KPP) in an Enterprise Information System (EIS) Value Assurance Framework (VAF)"* was prepared for The Office of the Undersecretary of Defense for Intelligence (OUSD(I)) and funded by OUSD(I).

Further distribution of all or part of this report is authorized.

This report was prepared by:

C.R. Gunderson
Research Associate
Information Science Department

Reviewed by:

Dan Boger, Chairman
Information Sciences Department

Released by:

Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Enterprise Information System (EIS) Value Assurance Framework (VAF) is an Information Technology (IT) governance model based on commercial best practice adapted to specific DoD and Intelligence Community (IC) acquisition policy requirements. VAF expands and abstracts traditional DoD "Availability" metrics such as "Operational Availability" A_o to develop objective time-based Key Performance Parameters (KPP) appropriate for software-intensive systems of systems. In particular VAF addresses both the DoD "Sustainment KPP" (S-KPP) and the "Net-Ready KPP" (NR-KPP). Hence, VAF provides an engineering assurance model for developing systems that deliver sustainable information superiority. In the VAF construct, the NR-KPP correlates measurable improvement in "Information Processing Efficiency" (IPE) to measurable improvement in traditional operational effect metrics such as Probability of Kill (Pk). In addition to that focus on operational efficiency, VAF recognizes that sustainment of modern IT systems requires process-level metrics that enforce speed-to-capability requirements. Hence VAF S-KPPs specify both threshold and objective speed-to-capability requirements commensurate with "Moore's Law." To achieve aggressive speed-to-capability, the VAF S-KPPs emphasize re-use of pre-certified COTS and GOTS components. The VAF addresses both of these types of KPPs through a recommended iterative process, consisting of 10 steps. Applying this process to a notional coalition counter-insurgency mission thread demonstrates its viability.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

EXECUTIVE SUMMARY

The Enterprise Information System (EIS) Value Assurance Framework (VAF) is an Information Technology (IT) governance model based on commercial best practice adapted to specific DoD and Intelligence Community (IC) acquisition policy requirements. VAF expands and abstracts traditional DoD "Availability" metrics such as "Operational Availability" A_o to develop objective time-based Key Performance Parameters (KPP) appropriate for software-intensive systems of systems. In particular VAF addresses both the DoD "Sustainment KPP" (S-KPP) and the "Net-Ready KPP" (NR-KPP). Hence, VAF provides an engineering assurance model for developing systems that deliver sustainable information superiority. In the VAF construct, the NR-KPP correlates measurable improvement in "Information Processing Efficiency" (IPE) to measurable improvement in traditional operational effect metrics such as Probability of Kill (Pk). In addition to that focus on operational efficiency, VAF recognizes that sustainment of modern IT systems requires process-level metrics that enforce speed-to-capability requirements. Hence VAF S-KPPs specify both threshold and objective speed-to-capability requirements commensurate with "Moore's Law." To achieve aggressive speed-to-capability, the VAF S-KPPs emphasize re-use of pre-certified COTS and GOTS components. The VAF addresses both of these types of KPPs through a recommended iterative process, consisting of the following 10 steps::

1. Establish a goal for a threshold-level improvement in operational performance based on ability to deliver within targeted short deployment time window.
2. Analyze the as-is information solution architecture including DOTMLTF.
3. Using that analysis, parametrically model the as-is Information IPE accordingly and calculate the current parameter values.
4. Model how operational performance depends upon IPE
5. Identify the incremental IPE improvement required to achieve the goal of threshold improvement in operational performance
6. Calculate the associated threshold target NR-KPP "Information Value Availability" (A_{iv})
7. Analyze options, define constraints, and design an appropriate solution architecture
8. Rapidly deliver incremental improvement
9. Test and certify the improved system against the goal NR-KPP A_{iv} to verify that the threshold improvement has been attained
10. Iterate the process from step 1.

Applying this process to a notional coalition counter-insurgency mission thread demonstrates its viability. I illustrate that in paragraph 4.

I. INFORMATION VALUE-BASED SUSTAINMENT KPP AND NET-READY KPP LINKAGE

The Enterprise Information System (EIS) Value Assurance Framework (VAF) is an IT acquisition governance model. VAF is based on modern commercial best practice and government best practice. It includes a suite of metrics derived from policy and guidance set forth in Defense directives such as references (a)-(d). VAF provides an implementation methodology for the recommendations of the Defense Science Board per reference (e).

The VAF recognizes that two of the mandatory KPPs described in reference (a) must be tightly coupled. These KPPs are the "Sustainment" KPP (S-KPP) and the "Net-Ready" KPP (NR-KPP).

Per reference (a), programs will typically field capability at threshold values of KPPs. They will employ a sustainment strategy to iterate toward eventually achieving objective values of KPPs. The Sustainment KPP is the formally mandated assurance model for achieving this continuous improvement through a series of above-threshold changes.

Per references (a)-(d), the NR-KPP objectively defines improvements in operational effectiveness enabled by information exchanges across EIS and National Security Systems (NSS). Certainly, any software-intensive IT system -- let alone any system tied to military operational effectiveness -- needs a sustainment model that assures continuous improvement throughout its lifetime. Reference (e) emphasizes this point and identifies speed-to-capability as arguably the greatest risk factor associated with DoD IT system acquisition.

Hence, a program's Sustainment KPP must be linked to its NR-KPP. In other words, the S-KPP must assure continued improvement in operational effectiveness enabled by effective information exchanges across IT and NSS systems.

II. INFORMATION VALUE-BASED NET-READY KPP FORMULATION

Per references (a) – (d), the NR-KPP has two parts:

1. Testable performance targets re mission effectiveness
2. Testable performance targets re information exchanges

Hence, the VAF factors NR-KPP into two parts:

1. Delivered Information Value (DIV)
2. Information Processing Efficiency (IPE)

such that:

$$A_{iv} = IPE \times DIV$$
$$IPE = (VB \div TB) \times W_P$$
$$DIV = P_1 \times P_2 \times \ldots . \times P_n$$

where:

A_{iv} = Information Value Availability
IPE = Information Processing Efficiency
- VB = Valued Bits Processed
- TB = Total Bits Processed
- W_P = Perishability factor, i.e. describes time window of utility

DIV = Delivered Information Value
- $P_1, \ldots, P_n$ = Measured or target scores re operational performance, e.g., Probability of Kill, Planning Cycle Time, Logistics Latency, etc.

Successful application of this methodology requires what is known in the IT industry as a "Beta" community. Beta communities are usually tech-savvy customers who are eager to work with early versions of new capability to help providers address their needs. The VAF approach adapts the concept of "Communities of Interest" (COI) identified in DoD GIG policy for this purpose. In the VAF construct COIs become hands-on beta development communities. These Beta COIs must include both members of the appropriate government operational community as well as relevant COTS developers. This approach both leverages COTS economy of scale and nudges COTS development in directions useful to the government. Programs can write contracts that require and enforce such beta community creation and involvement.

The VAF develops IPE in context with DIV. IPE is a measure of "semantic interoperability", i.e. how easily and effectively disparate data from disparate sources on network(s) are collected and bundled usefully together. This formulation requires that semantic interoperability be designed, built, and tested against specific desired outcomes, rather than in the abstract. Specifically, to implement semantic interoperability follow the following procedure repeated verbatim from the executive summary for the readers' convenience:

1. Establish a goal for a threshold-level improvement in operational performance based on ability to deliver within targeted short deployment time window.
2. Analyze the as-is information solution architecture including DOTMLTF.
3. Using that analysis, parametrically model the as-is Information IPE accordingly and calculate the current parameter values.
4. Model how operational performance depends upon IPE
5. Identify the incremental IPE improvement required to achieve the goal of threshold improvement in operational performance
6. Calculate the associated threshold target NR-KPP "Information Value Availability" (A_{iv})
7. Analyze options, define constraints, and design an appropriate solution architecture
8. Rapidly deliver incremental improvement
9. Test and certify the improved system against the goal NR-KPP A_{iv} to verify that the threshold improvement has been attained
10. Iterate the process from step 1.

DIV might be based on a goal level of improvement, e.g., $P_{Pk} = 1.1$ could represent a target of 10% improved Probability of Kill (Pk) where "1.0" is the normalized index of the current Pk.

IPE is in two parts, a value ratio (VB/TB) and a perishability factor.

The value ratio might formulated as:

$$VR = AB \div TB$$

Where:

VR = Value Ratio
AB = Actionable Bits,
TB = Total Bits Processed

Notice that in this example "Valued Bits" (VB) are defined as "Actionable Bits" (AB). Actionable Bits are those that stimulate a change to planned actions, either to avoid a threat or capitalize on an opportunity.

Pk is likely to be highly correlated to the latency of exchange of critical target location information. That said, Pk has a practical limit of less than 100%. Further, there are latencies associated with some mission thread transactions that don't have anything to do with IPE. Recognizing those limitations to the model, we might formulate the perishability factor as a piecewise linear function of information exchange latency that closely resembles Pk as a function of the same latency as follows:

$$W_P = 1 \text{ if } L \leq L_O;$$
$$W_P = 0 \text{ if } L > L_T;$$
$$W_P = (L_T - L)/(L_T - L_O) \text{ if } L_O < L < L_{T'};$$
$$W_P = (W_P)_T \text{ if } L' \geq L \leq L_T$$

Where:

W_P = Perishability weighting factor as a function of latency
$(W_P)_T$ = Perishability weighting function assigned to L_T
L = Information exchange latency
L_O = Objective value of information exchange latency
L_T = Threshold value of information exchange latency
$L_{T'}$= Information exchange latency linearly correlated with $(W_P)_T$

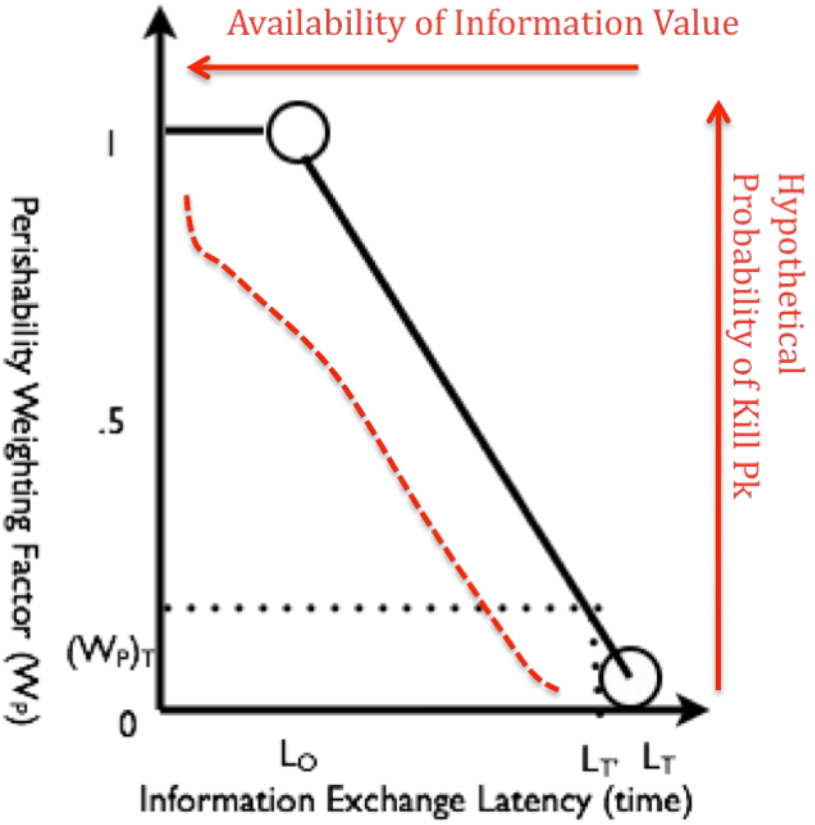

Figure 1: If Probability of Kill is correlated with latency for receipt of critical locating information, we can use the correlation to model a perishability weighting function. L_O is the objective and L_T is the threshold value for information exchange latency. The availability of information value A_{iv} increases as L decreases and Pk increases.

In figure 1, L_O and L_T correspond to objective and threshold values of Pk. The perishability factor W_P remains at its maximum value of 1 if information exchange latency is at or better than objective value. As latency increases toward the threshold value, W_P decreases linearly to the value of assigned to the L_T ($(W_P)_T$). W_P, and hence A_{iv}, goes to zero as latency exceeds the threshold value.

III. INFORMATION VALUE-BASED SUSTAINMENT KPP FORMULATION

Per reference (a), the S-KPP and its supporting Key System Attributes (KSAs) address three closely related themes:

1. Testable "Material Availability", *i.e.* total up time divided by total down time per reference (a).
2. Testable Reliability, i.e. likelihood that system will not fail during a specific time interval. Often calculated with Mean Time Between Failure (MTBF).
3. Testable Ownership Cost, *e.g.* investment required to maintain reliability and to provide for continuing improvement throughout the system's life.

Applying the S- KPP and KSAs to a software-intensive, widely distributed, IT system of systems is problematic. Traditional approaches are designed for hardware "boxes" wherein overall system availability, reliability, and ownership costs are bounded by the components in the "box" of interest. The nature of "cloud" and "service oriented" network architectures deliberately abstracts the detail of component level performance away from the over-all system performance. If a box on a server farm fails, the failure is unlikely to impact service availability. On the other hand, if a demand spike exceeds server farm capacity, service availability will suffer even if all components function properly. Further, traditional hardware reliability measures and prediction models are not suited for software, and "reliability" metrics designed for software are immature.

"Operational Availability" (A_o) is a traditional system-level metric often used as a KPP. A_o addresses run-time availability. Generally, A_o is "up time" divided by "up time" + "down time." Specifically, A_o is a model of availability that employs Mean Time Between Failure (MTBF), Mean Time to Repair (MTTR), and Mean Logistics Delay Time (MLDT), such that:

$$A_o = MTBF/(MTBF + MTTR + MLDT)$$

If a part is hard to repair, or takes a long time to obtain, the program manager (PM) might decide to provide an on-board spare or even a hot-spare. This will probably increase cost, but an alternative approach to develop a more reliable component may cost even more and add risk to the schedule. Programs must make risk-benefit decisions about how to achieve required run-time performance – *i.e.* a specified value of A_o -- with objective quantification of cost and schedule.

Success with Internet "cloud" and "service oriented" architectures requires a system-of-systems perspective. We need processes to help optimize the myriad

options re technology, architecture, IPR, contract vehicles, bundling options, test and certification models, etc.

Reference (e) (as well as myriad GAO reports and articles in the press) identifies speed-to-capability as a critical failing in the DoD acquisition process. Accordingly, VAF addresses this issue by providing metrics that, in addition to run-time availability, focus on "availability" over development and delivery schedule as well as operation time. That is, VAF introduces process-level metrics that focus on build-time efficiency. The time limiting factor for fielding IT is, at least notionally, Moore's Law. A new generation of IT evolves every 18 months or so. VAF KPPs acknowledge that fact as a boundary condition, where development and delivery together must be at least as fast as the generational rate of 18 mos.

The VAF speed-to-capability process metric is called "Net Ready Availability" (A_{nr}). A_{nr} is a parameterization of the S-KPP that is analogous to A_o, but treats the acquisition process itself as within the boundary of the system of interest. In fact, the acquisition process is the part of the overall system responsible for delivering continuous improvements. VAF formulates A_{nr} as follows:

$$A_{nr}(t) = T_D(i)/T_{CD}(c)$$
$$T_{CD}(c) = T_D(c) + T_T(c) + T_c(c)$$

Where:
$A_{nr}(t)$ = Net Ready Availability as a function of time
$T_D(i)$= Initial estimate of development time, a constant
$T_{CD}(c)$ = Current estimate of capability deployment time, a variable with respect to time
$T_D(c)$ = Current estimate of development time, a variable with respect to time
$T_T(c)$ = Current estimate of post-development test time, a variable with respect to time
$T_c(c)$ = Current estimate of post-test certification time, a variable with respect to time

We can further break out components of T_D as follows:

$$T_D = T_I + T_R + T_B + T_O$$

Where:

T_I = Invention Time, *i.e.* time required for creation of new intellectual property
T_R = Re-invention Time, *i.e.* time spent developing capability from scratch that already exists on the shelf.

T_B = Bundling Time, *i.e.* time expended harvesting capability through the build-time interoperability (composability) of Net-Ready components
T_O = Overhead Time, *e.g.* redundant paperwork

We can add weighting functions to emphasize various best practices such as keeping software up to date. For example:

$$W_{sc} = SC/(LOC/BLOC)$$

Where:

W_{sc} = Software currency weighting factor. W_{sc} increases as programs upgrade to current software products and standards and sunset legacy code.
SC = Software Currency, *e.g.* SC = 1 if code is within one build, patch, architecture, standard, etc. of the most current. SC = 0.1 if otherwise.
LOC = Current count of Lines of Code
BLOC = Baseline count of Lines of Code

To apply A_{nr}, programs first must recognize that they need to deploy capability quickly, say between 12 and 36 months. Programs then plan to deliver a capability portfolio scoped for delivery within that 12- 36 month "Capability Deployment Time" (C_{DT}) window. The scoping might allow for some newly "invented" components, but it will mostly require re-using pre-certified COTS or GOTS components.

In this model, the acquisition strategy is to incentivize developers to "re-use" capability, i.e. bundle, pre-certified off-the-shelf components. Developers will deliver several interim test bundles within the T_{CD} window and adjust their schedules after each iteration. Their goal is to deliver as much useful capability as possible, but to meet delivery schedule at all costs. If the schedule is at risk, *i.e.* the current estimate of T_{CD} (c) in the denominator increases, the value of A_{nr} (t) decreases. If A_{nr} decreases below some established threshold, the developers must adjust to meet the speed-to-capability imperative. Thus, programs avoid fielding obsolete capability. See Figure 2.

The VAF process seeks to decrease Overhead Time (T_O) by reducing redundant paperwork. For example, today there are a hundreds of policy documents governing various aspects of government IT acquisition. VAF-based testers can apply semantic technologies to capture the overlapping essential objective elements of policy, and to identify and resolve any conflicting policies. Likewise, multiple IT programs have many overlapping basic requirements. Today those programs each capture redundant requirements in expensive paper artifacts. Again, testers can use semantic technology to capture requirements in machine -

readable formats. This approach allows programs to efficiently re-use pre-validated requirements artifacts.

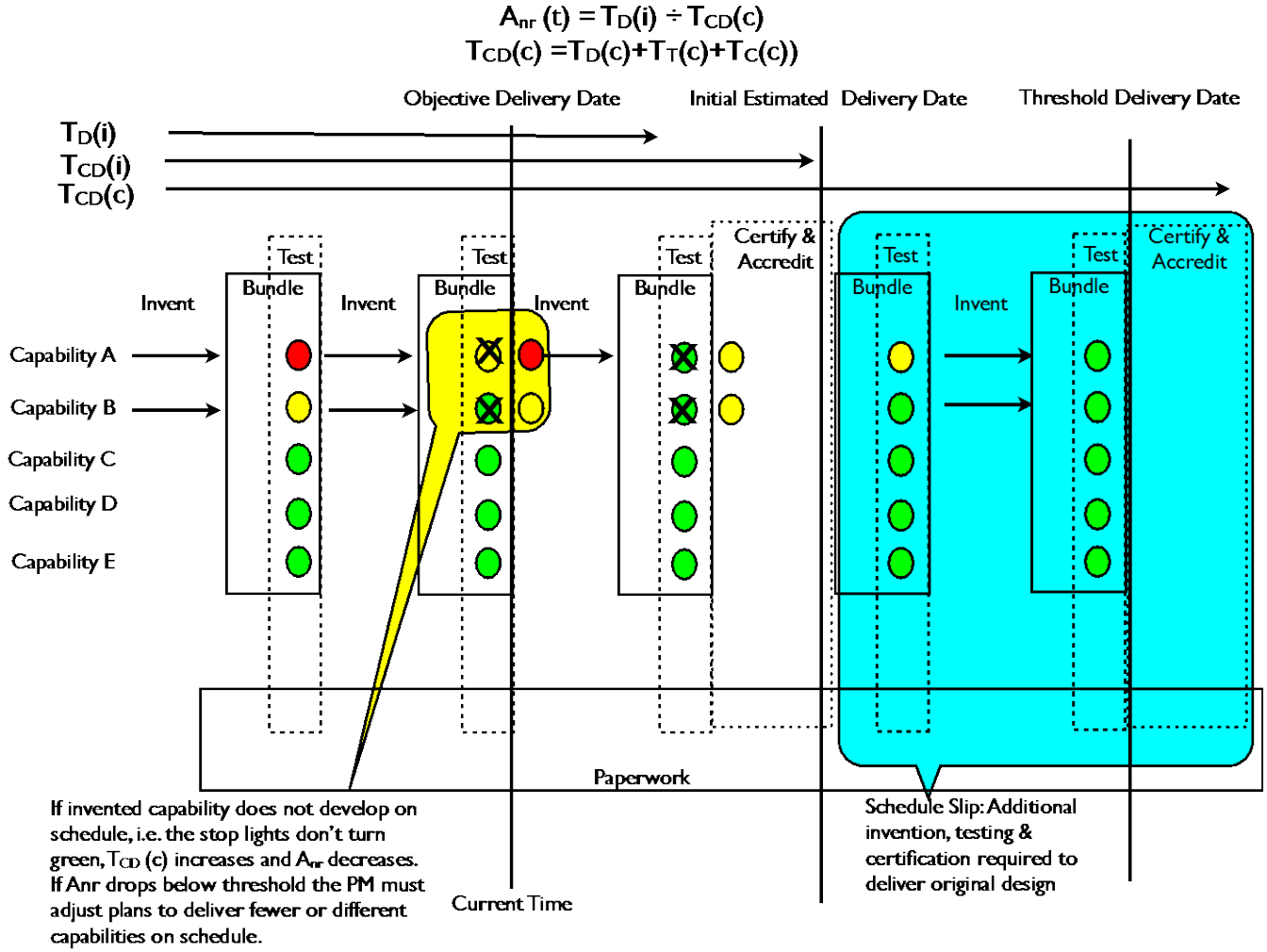

Figure 2: Net-Ready Availability" (A_{nr}) is an S-KPP based on speed-to-capability. A_{nr} compares initially scheduled development time (T_D) to the current estimate of capability deployment time (T_{CD}). T_{CD} is equal to T_D + any additional time required for test (T_T) and certification (T_C). This approach considers the capability delivery date to be an aspect of the KPP with established objective and threshold values. A PM's strategy is to reduce risk to schedule by bundling only small increments of newly "invented" specialized capability with existing pre-certified off-the-shelf capabilities in frequent spirals.

"Modularity", "interoperability", and "portability" are all attributes associated with re-usability and bundling. These attributes have historically been difficult to measure and enforce. Historically "chasing standards" has not generally helped. Further, DoD has traditionally interpreted the mandate for "interoperability" to require new systems to be backward compatible with fielded systems. The VAF approach suggests a paradigm shift. The new paradigm requires that fielded systems maintain "forward interoperability" by staying abreast of emerging mainstream commercial technology. Accordingly, VAF suggests that NR-KPP certifiers stop specifying and verifying compliance with universal standards. Rather, they should:

(1) Work closely with commercial standards' bodies[1] to:

(a) Articulate government objectives and address them continuously within the commercial standards development process.

(b) Develop a government certification model for the commercial IT standards development process based on agreed best practices re speed, rigor, and "openness".

(2) Certify the standard bodies' processes (per j.1.b) rather than certifying each new standard. That is, certifiers should immediately accept the most current standards published by certified standard bodies as "authoritative."

(3) Certify that programs' sustainment models can credibly perform technology refresh on pace with emergent commercial standards throughout system life cycle.

Having designed their NR-KPP/S-KPP-compliant solutions architecture, programs will choose specific standards, off-the-shelf products, licenses, and contract models accordingly. They will consider options for operating systems, middleware, messaging, registry, discovery, etc. Trade-off analysis is analogous to that performed in the traditional A_o model. However, now programs will optimize for both S-KPP speed-to-capability and NR-KPP information-value-delivery requirements.

VAF focuses on demonstrated ability to bundle components. "Bundle-ability" corresponds to how quickly and easily modular components can be assembled for new uses. In that sense, "bundle-ability" is equivalent to "reusability." Reusability is equivalent to build-time interoperability. Hence, S-KPP/NR-KPP-based certification will document programs' reuse of components, and the reusability of their newly developed components. The documentation will include description of specific value added to mission outcomes. The process will populate an approved products list of reusable components. Certifiers will help programs through the process by helping them to select appropriate open commercial standards and associated approved products.

[1] Over the last 20 years, the groups contributing to productive IT "standards" have broadened to include open source groups such as IETF, Linux, W3C, FSF, and commercial keiretsu such as OASIS, TOG, MISMO, RosettaNet, etc. Many of the most useful standards are now considered mere "recommendations" by their producers. Thus, the DoD must broaden its sense of standards to embrace emerging recommendations from important de facto standard setters. Even a monopolist such as Microsoft or a dominant player such as Oracle can impose de facto standards on the marketplace that the government should deliberately exploit.

IV. INFORMATION VALUE-BASED SUSTAINMENT KPP/NR-KPP USE CASE

Consider how VAF might support the following notional coalition counter-insurgency mission thread. Note that this example is over-simplified for clarity.

US1 is a US National cell that performs Command and Control (C2) for US forces involved in coalition counter-insurgency operations.

US1 receives ad hoc "tipper" information regarding the location of High-Value Targets (HVT) over a TOP SECRET Internet Protocol (IP) network from the US-only surveillance and reconnaissance process. This information is generally not actionable unless it is corroborated by an "authoritative source."

US1 subscribes to a ten-element intelligence report from Coalition Intelligence Processing Center (CIPC). CIPC is an authoritative source of counter-insurgency intelligence.

CIPC refreshes its intelligence report every hour and delivers it via a classified Coalition IP network.

US1 typically takes 15 minutes to process the CIPC report.

If the CIPC report corroborates the tipper information, US1 issues "kill" orders to US2 via a Classified US-only IP C2 network. US2 is a US National unit that performs targeting and weaponeering.

US2 collects and shares information via various classified and unclassified tactical links, push-to-talk radios, and IP networks.

US2 typically requires 15 minutes to prepare targeting artifacts, select best available weapons and platforms, and forward kill orders to selected coalition platforms.

Coalition forces might need anywhere from a few minutes to an hour to engage the target.

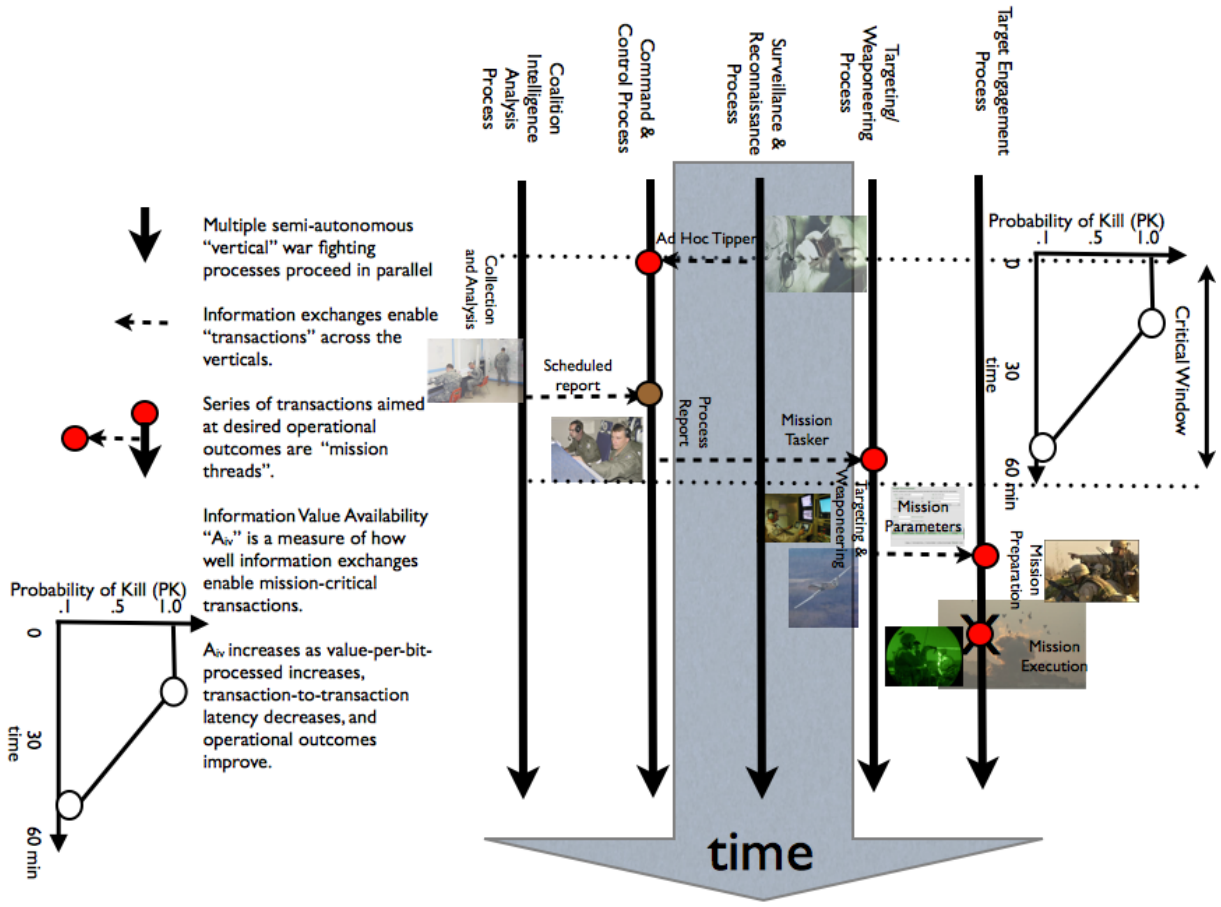

Figure 3: "Information Value Availability" (A_{iv}) is a formulation of the NR-KPP that quantifies "semantic interoperability." The objective of semantic interoperability across an enterprise is to enable powerful transactions among loosely coupled verticals. In this example the "enterprise" is a military coalition. The "verticals" are various war fighting processes. Myriad communications circuits provide the loose coupling. Few, if any, of these circuits are shared across all the verticals. Likewise, trust models vary with processes, participants, and situations. A_{nr} constrains evolving information architectures to selectively exchange and process the most critical data bits, decrease latency of critical information exchanges, and improve critical operational outcomes measurably.

We apply the ten-step VAF process introduced in paragraph 2.c. above.

1. Performance goal:

   The operational beta community seeks a 100% improvement (*i.e.*, 2 X) in Pk within 18 months, and 10% per year thereafter. This requirement translates to a threshold Delivered Information Value (DIV_T) value of:

$$DIV_T = 2 \text{ X } Pk_{Baseline}$$

2. Analyze as-is architecture:

Figure 4 sketches the notional mission thread transactional architecture.

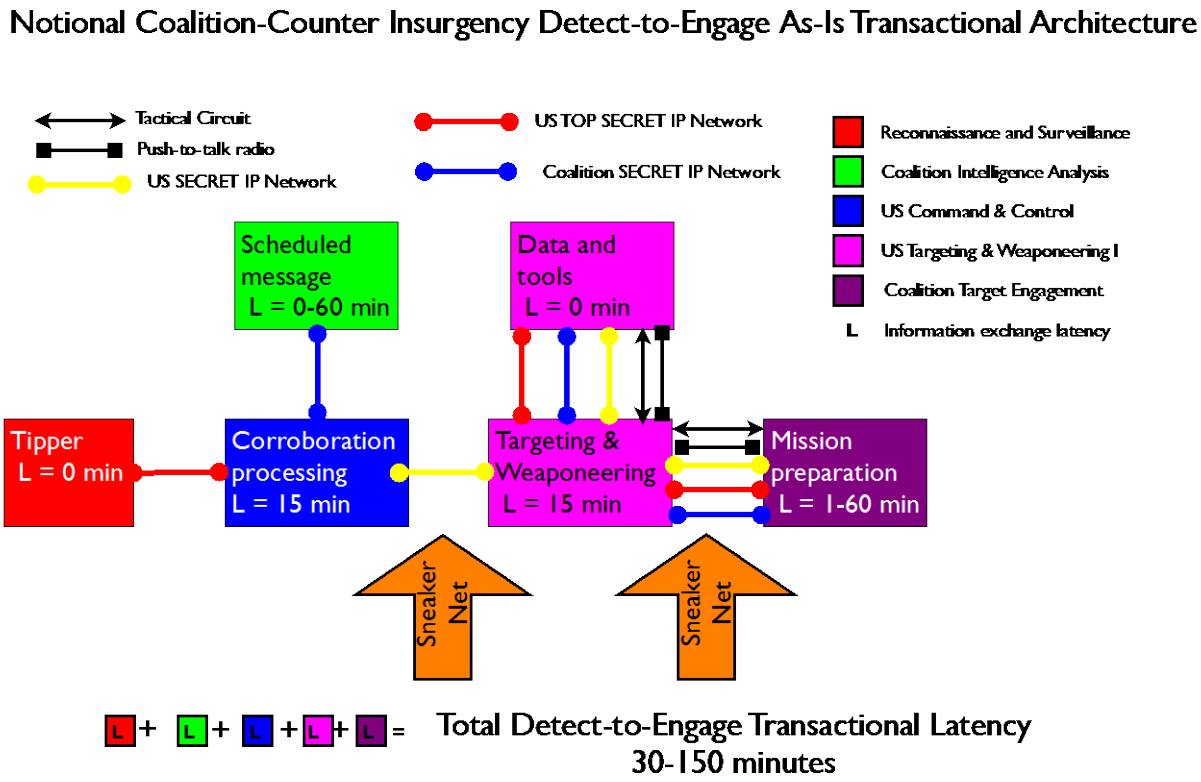

Figure 4: Hypothetical legacy architecture includes a collection of non-interoperable communications enclaves and non-integrated information processing activities. Consumers must pull out the information they consider most critical from large volumes of data that is relatively crudely sorted. Cross-process collaboration in this enterprise often requires that a trusted broker "sneaker net" sanitized information from one proprietary communications circuit to another. Hence, the enterprise lacks agility to routinely close critical transactions in time.

The C2 process hypothetically initiates the mission thread when US1 receives a "tipper" about the location of an HVT from the Reconnaissance and Surveillance process. Beta community experts explain that getting confirmation of the tipper information from an authoritative source is the most critical information exchange. They confirm that in the as-is scenario US1 performs this confirmation by processing the intelligence summary they receive from CPIC.

Recall that the CPIC prepares and delivers this summary message every hour. US1 requires fifteen minutes to process the message and extract any corroborating information. Therefore, total latency for this information exchange is from 15 to 75 min.

The hypothetical operational Beta community experience shows that tipper information is very perishable. HVTs normally re-locate within sixty minutes of reported sightings.

On the other hand, (hypothetically) the tipper information, when corroborated, has proven to be very accurate. Likewise, coalition weapons platforms have proven to be highly lethal.

Given the existence of a corroborated tipper, its accuracy together with coalition force lethality, has proven Pk to be an almost linear function of detect-to-engage mission thread transactional latency information exchange time latency.

Beta community experts estimate that detect-to-engage times of 10 and 60 minutes would correspond to Pk of almost 100% and 10% respectively.

These experts explain that their current baseline for Pk, given a corroborated tipper, is on the order of 10%. Hence, we will assume baseline Pk = 10%.

CPIC does not have authorization to receive the tipper information directly from the TOP SECRET US-ONLY network. If it did, CPIC could immediately corroborate the tipper with its other sources. Operational experts explain that, although collected through TOP SECRET sources, the tipper information itself is so perishable that sharing it presents relatively little risk.

The operational Beta development community explains that the US2 targeting and weaponeering process uses operational reconnaissance assets such as Unmanned Aerial Vehicles (UAV) to put “eyes-on-target” and calculate precise weapon delivery coordinates. US2 communicates with UAVs over unclassified proprietary point-to-point links.

US2 uses many tools and circuits, including Blue Force Tracker (BFT) via an unclassified commercial satellite link, to locate candidate weapons and delivery platforms. Depending on which platforms and weapons it chooses -- *e.g.* Predator UAV and Hellfire missile, or SEAL Team and sniper rifle -- US2 uses a variety of communications paths to deliver a “9 line” targeting parameter message to the weapon delivery platform.

3. Calculate baseline IPE:

Recall that IPE is in two parts, a “value ratio” and a perishability factor.

$$IPE = VR \times W_P$$

We calculate the value ratio for the CPIC-to-US1 corroboration information exchange as follows:

$$VR = AB \div TB$$

Where:

VR = Value Ratio
AB = Actionable Bits,
TB = Total Bits Processed

The information exchange associated with corroboration is a ten-section message. Only one of the sections contains exchanged message has actionable bits. Therefore, approximately:

$$VR = 1 \div 10 = 0.1$$

Operators confirm that although they spend all of their time collecting and analyzing information, no more than 10% of that information turns out to be actionable. The rest of the data they process either confirms their current understanding, adds to their general situational awareness, or is useless. (Obviously this is a very crude example of how to calculate value-per-bit-processed. However, the VAF approach will quickly iterate empirically toward a pragmatically useful, empirical, measure. Therefore, it is not vital to start with a precise baseline index. It <u>is</u> vital that the operational customer community vouches for the value and utility of the approach.)

Now we model W_P as explained in paragraph 2.c. Based on hypothetical operational Beta community input above, set the objective value for information exchange latency at L_O = 10 minutes and the threshold at L_T = 60 minutes. Assign $(W_P)_T = 0.1$ to L_T = 60 minutes. Calculate $L_{T'}$:

$$(W_P)_T = 0.1 = (60 - L_{T'})/(60\text{-}50)$$

$$L_{T'} = 55 \text{ min}$$

Now we can specify the weighting function as follows:

$$W_P = 1 \text{ if } L \leq 10 \text{ min};$$

$W_P = 0$ if $L > 60$ min;
$W_P = (60 - L)/50$ if 10 min $< L <$ 55 ;
$W_P = .1$ if $55 \geq L \leq 60$ min

Where:

W_P = Perishability weighting factor
L = Information exchange latency

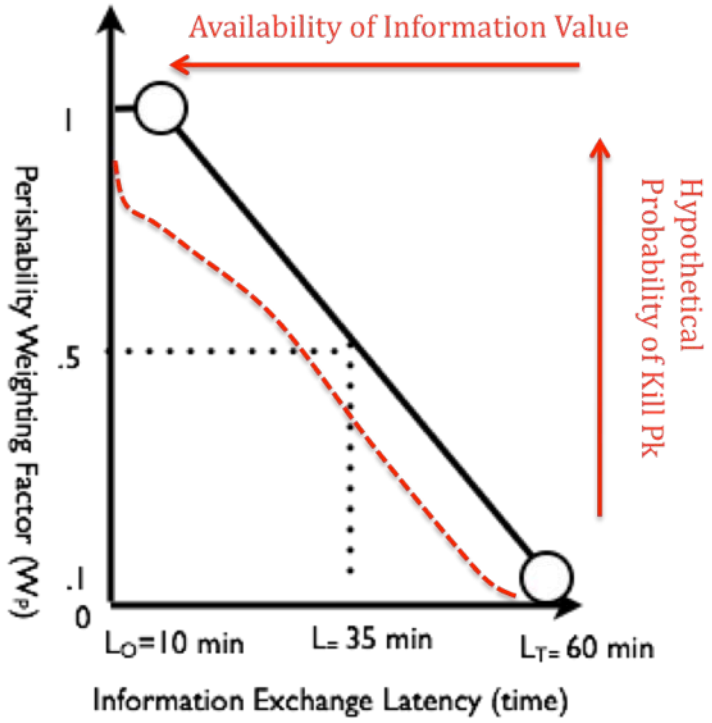

Figure 5: (Hypothetical) operators explain that given the existence of corroborated locating information for High Value Targets (HVT), Probability of Kill (Pk) depends almost exclusively on the latency (L) of the essential information exchanges. They believe a Detect-to-Engage transactional latency of 10 minutes or less corresponds to an almost 100% Pk. On the other hand, the HVTs tend not to stay in one location for more than an hour. Hence latencies of greater than 60 minutes correspond to Pk = 0.

Per step #2, $Pk_{Baseline}$ = 10%. Per discussion in step 3 (above) Pk=10% corresponds to a value of W_P of 0.1

$$IPE = .1 \times W_P$$

$$IPE_{Baseline} = .1 \times .1 = .01$$

4. Model dependency of operational performance to IPE:

Pk = f(IPE) = f(AB, L) such that Pk increases as: (a) Actionable Bits (AB) are available; and (b) Actionable Bits are exchanged and processed quickly. In other words Pk is strongly positively correlated to IPE as follows:

$$Pk \approx K \times IPE$$

Where:

K = Proportionality function. Using the baseline values calculated above we solve for K:

$$Pk_{Baseline} \approx K \times IPE_{Baseline}$$

$$.1 \approx K \times 0.01$$

$$K \approx 10$$

Operators confirm that based on their experience it is reasonable to assume that Pk is linearly related to IPE. Therefore we assume initially that:

$$Pk \approx 10 \times IPE$$

5.Identify incremental IPE improvement goal:

Per step 1, the threshold performance improvement goal is a 2 X improvement in PK. Per step 2, $PK_{Baseline}$ = 10%. Per step 4, Pk = 10 X IPE. Therefore the threshold IPE improvement goal (IPE_T) is:

$$Pk_T = 2 \times Pk_{Baseline} = 2 \times .1 = .2$$

$$IPE_T = Pk_T/10 = .2/10 = .02$$

6.Calculate A_{iv} threshold value:

$$(A_{iv})_T = IPE_T \times DIV_T$$

Where:

$(A_{iv})_T$ = Threshold value of Information Value Availability
IPE_T = Threshold value of Information Processing Efficiency
DIV_T = Threshold value of Delivered Information Value

Per step 1 the $DIV_T = 2 \text{ X } Pk_{Basline}$. Per step 2, $Pk_{Basline} = 10\%$. Therefore:

$$DIV_T = 2 \text{ X } 0.1 = 0.2$$

Per step 5, $IPE_T = 0.02$. Therefore:

$$(A_{iv})_T = 0.2 \text{ X } 0.02 = .004$$

7. Analyze options and constraints. Design solution architecture:

The mission thread consists of four critical serial transactions.

1. Exchange information to identify and confirm target location
2. Exchange information to select weapons and platforms.
3. Exchange information to launch attack.
4. Deliver ordinance to kill target

Operational effectiveness, *i.e.* Pk in this case, depends on the accuracy of the information exchanges in transactions 1-3, the lethality of the ordinance delivery in transaction 4, and the collective time it takes to close the 4 transactions. In this case, accuracy and lethality are not issues. The sole issue is transactional latency. Latency for exchanges 1-3 depends on IPE.

Per figure 4, the as-is mission thread employs five semi-autonomous processes and at least five different proprietary communications paths. No communication path is common to all five processes.

There is no shared trust model across the five processes.

Per the discussion above, a solution architectural strategy is as follows:

Requirement: Build as much capability as possible with COTS and GOTS components. Continuously deploy incremental improvements. A specific requirement is to develop GOTS sensor services for UAVs and other platforms. Work closely with the customer community.

Solution: Employ SOA. USE COTS SOA middleware. Use COTS geospatial services. Re-use GOTS “track” services (*e.g.* WEB COP.) Develop GOTS UAV sensor service. Use

GOTS security services. Write procurement contract language to require lifecycle technology refresh, and Beta community feedback.

$$A_{nr}(t) = T_D(i)/T_{CD}(c) \text{ X } W_{SC}$$

$$T_{CD}(c) = T_D(c) + T_T(c) + T_c(c)$$

$$T_D = T_I + T_R + T_B + T_O$$

W_{sc} = SC/(LOC/BLOC) = 1 per procurement requirement

A_{nr} = 12 mos / (6 + 0 + 4 + 2 + 3 + 3) mos x 1 = .66

Requirement: Provide common communication backplane. In this case, a specific requirement is for a routable network.

Solution: Use commercial Internet Service Provider (ISP) for shared UNCLAS Internet access. Long-term target is "black core" Multi-Level Security (MLS) from UNCLAS to TS.

Requirement: Develop policy-based trust model. In this case a specific requirement is to develop need-to-share policy and services to enable restricted tipper information to flow directly from surveillance and reconnaissance process to coalition intelligence analysis process.

Solution: Employ Multiple Independent Layers of Security (MILS) architecture. Reuse pre-certified GOTS IA authorization and authentication service components. Begin at UNCLAS level and then spiral toward multi-level security. Work with Beta-test community to invent dynamic need-to-share and "unanticipated user" IA release policy.

Requirement: Reduce "information overload". Reduce the number of critical transactions per mission thread and close them more quickly. A specific requirement, in this case, is to capture track information for both coalition weapon platforms and HVTs in machine-readable information exchange models (IEM). The IEM must enable automated, policy-based, weapon-target pairing and tasking.

Solution: Reuse relevant target tracking information model components to describe and share target and weapon platform information. Work with beta community to invent

"Critical Conditions of Interest" VIRT information exchange requirement profiles to focus exchanges on HVT information components

8. Rapidly deliver incremental improvement:

For this mission thread example, assume the incremental improvement included:

- UNCLAS Internet connectivity across the coalition
- Dynamic need-to-share services
- Alert service for the HVT scenario
- Track service
- UAV visual sensor services

This type of development has previously proved successful. Specifically, the Coalition Warrior Interoperability Demonstration (CWID) 08 Interoperability Trial (IT) 5.64 (see reference (f)) demonstrated a similar high assurance tactical SOA stack developed with GOTS and COTS components in twelve months. Their approach was as follows:

- Base IT procurement in acquisition components that can reduce risk re cost, performance, and schedule
  - Exploit new GIG acquisition policies
  - Extend and expand pure COTS competition
  - Issue simple use cases in lieu of traditional RFI/RFP
  - Require mission context prototypes vice paper studies
  - Shorten delivery cycles and contract review periods
  - Exercise government purpose rights to software licenses
- Incentivize PMs and COTS vendors to participate
  - Furnish pre-approved GOTS components
  - Streamline Certification and Accreditation (C&A)
  - Furnish V&V to put COTS on approved products list

9. Test and certify against A_{iv}:

In our hypothetical case, NR-KPP certifiers would solve for A_{iv} in the new solution architecture:

$$(A_{iv})_T = IPE_T \times DIV_T$$

Consultation with experts, campaign models, or other customer-approved methods will return the new predicted value of Pk. In this

case, Delivered Information Value (DIV) is exactly equivalent to Pk. If the new tested value of Pk does not meet or exceed NR-KPP threshold of $Pk_T = 0.20$, the system does not pass. Note that once the first increment of new capability has been fielded, we can use the actual operationally audited value of Pk in future spirals. For this example, arbitrarily assume:

$$Pk_{New} = 0.40$$

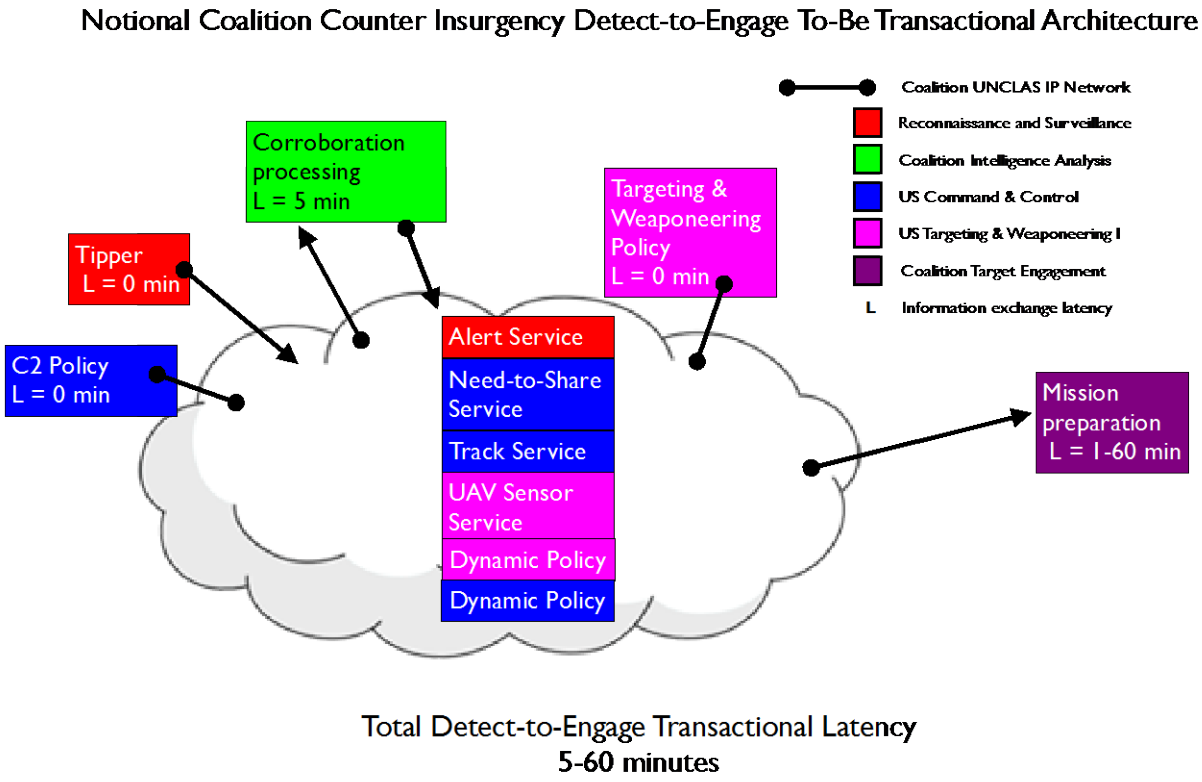

Figure 6: Hypothetical to-be architecture includes an Internet "cloud" with web service stack. Mission authorities continuously revise policy per commander's intent and emerging facts on the ground. Sensor services provide real-time situational awareness. High value targets (HVT) and Coalition weapon platforms are tracked with rich semantic models. Pre-identified critical conditions of interest trigger emergency action tasking messages. Need-to-share services allow access based on pre-determined policy regarding identity, role, and emergent situation on the ground.

Figure 6 describes the notional solution architecture outlined in step 7. If it this architecture is fielded as planned, we can calculate IPE as follows:

$$IPE = AB \div TB \times W_P$$

The only bits processed in this scenario are actionable – the alert service is designed to assure that. So, AB = TB and AB ÷ TB = 1. The transactional latency budget in the solution architecture

includes 5 minutes for corroboration and from 1 to 60 minutes for mission preparation. If we assume an average value of 30 minutes for mission preparation, the mean total transactional latency is L = 35 minutes. Entering the chart at Figure 5 with L = 35 returns W_P = 0.5. So:

$$IPE = 1 \text{ X } 0.5 = 0.5$$

Now we can solve for A_{iv}.

$$A_{iv} = IPE \text{ x } DIV = 0.5 \text{ x } 0.4 = .0.2$$

$$(A_{iv})_{New} = 0.20 > (A_{iv})_T = 0.004$$

Because A_{iv} exceeds the threshold value, NR-KPP certifiers accept the system and place the newly certified components on the approved products list.

At this point we can re-evaluate the modeled relationship between IPE and Pk for the next iteration. Previously we had modeled IPE as:

$$IPE = K \text{ X } Pk$$

Our original estimate was that K = 10. Per discussion above:

$$IPE = 0.5 = K \text{ X } 0.4$$

$$K = 0.5 \div 0.4 = 1.25$$

Apparently, IPE, in the new architecture, is even more closely correlated with Pk than our original model suggested.

Conceptually, given the order of magnitude improvement in A_{iv}, this notional solution architecture is very powerful. However, cartoon drawings of “clouds and arrows” can do anything. It may not be realistic to field an operational realization of the cloud and arrows within the eighteen-month goal of this hypothetical development effort. That said, fielding even a subset of the envisioned capability -- say the Internet backbone and a CONOPS-based need-to-share service -- might surpass the threshold NR-KPP requirements.

Returning briefly to the previously mentioned CWID 08 IT 5.64 demonstration. The analysis of that demonstration employed a test and certification model against a use case similar to the present example. Findings showed 20% improvement in Probability of

Detection of the target of interest; 100% improvement in Detect to Engage time; 60-200% improvement in IPE as a result of VIRT and Need-to-Share services.

10. Iterate:

    Repeat steps 1 – 9 with new target values for Aiv, IPE, and Pk.

LIST OF REFERENCES

(a) CJCSM 3170.01C. Operation of the Joint Capabilities Integration and Development System, 1 May 2007

(b) DODD 4630.5 Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 5 May 2004

(c) DoDI 4630.8**.** Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004

(d) CJCSI 6212.01 Interoperability and Supportability of Information Technology and National Security Systems, 15 Dec 2008.

(e) Defense Science Board (DSB) Report on DoD Policy and Procedures for Acquisition of Information Technology, Mar 2009

(f) CWID 08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2, presented to GMU/AFCEA May 2009

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943

4. ISR Programs
   Undersecretary of Defense for Intelligence
   Washington, DC